IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:16-CR-265
	)	
Plaintiff,	)	JUDGE JOHN R. ADAMS
	)	
v.	)	
	)	
	)	
	)	
	)	
ERICK JAMAL HENDRICKS,	)	
	)	
Defendant.	)	

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT'S PRETRIAL MOTION FOR DISCLOSURE OF FISA-RELATED MATERIAL AND TO SUPPRESS THE FRUITS OR DERIVATIVES OF ELECTRONIC SURVEILLANCE

JUSTIN E. HERDMAN
United States Attorney for the
Northern District of Ohio
Attorney for the United States of America

Matthew W. Shepherd
Assistant United States Attorney

Rebecca Magnone
Trial Attorney, National Security Division

Chad M. Davis
Attorney Advisor, National Security Division

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

U.S. CONSTITUTION

FEDERAL STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

The Government is filing this classified Memorandum in Opposition to the Defendant's Pretrial Motion for Disclosure of Foreign Intelligence Surveillance Act (FISA)- Related Material and to Suppress the Fruits or Derivatives of Electronic Surveillance (hereinafter Doc. 40 or defendant's motion). The defendant seeks: (1) disclosure of all FISA-related materials (*i.e.*, the FISA materials) and (2) suppression of the evidence derived from FISA electronic surveillance and any other means of FISA collection or foreign intelligence gathering (*i.e.*, FISA information). (Doc. 40 at 1).[1]

The defendant's motion has triggered this Court's review of the FISA materials related to the FISC-authorized electronic surveillance and physical search[2] to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval.[3] Whenever "a motion is made "to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under [FISA,] the United States district court . . . shall . . . if the Attorney

---

[1] **[CLASSIFIED MATERIAL REDACTED].**

[2] Although the defendant does not expressly challenge physical search, the Government has interpreted the defendant's challenge to "any other means of FISA collection" to include physical search because the Government provided notice to Hendricks and this Court that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained or derived from electronic surveillance and physical searches conducted pursuant to [FISA]." (*See* Doc. 20).

[3] The provisions of FISA that address electronic surveillance generally are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f); *see also* 50 U.S.C. § 1825(g). The Government is filing herewith such an affidavit in which the Attorney General claims under oath that disclosure or an adversary hearing would harm the national security of the United States, which is the prerequisite for the Court to review the FISA materials *in camera* and *ex parte*;[4] consequently, the Government respectfully submits that, for the reasons set forth hereinafter, this Court should conduct an *in camera, ex parte* review of the documents relevant to the defendant's motion in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).[5]

The Government respectfully submits that, for the reasons set forth below, and as the Court's *in camera, ex parte* review will show: (1) the electronic surveillance and physical search at issue were both lawfully authorized and lawfully conducted in compliance with FISA; (2) disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the electronic surveillance and physical search without disclosing the FISA materials or portions thereof; (3) the FISA information should not be suppressed; (4) the FISA materials should not be disclosed; and (5) no hearing is required.

---

[4] The Attorney General's affidavit ("Declaration and Claim of Privilege") is filed both publicly and as an exhibit in the Sealed Appendix to this classified filing. *See* Sealed Exhibit 1.

[5] **[CLASSIFIED MATERIAL REDACTED].**

A. BACKGROUND

On August 17, 2016, Erick Jamal Hendricks (Hendricks) was charged by indictment in the Northern District of Ohio with one count of conspiracy to provide material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B (a)(1). (*See* Doc. 7). On December 13, 2016, a superseding indictment was returned, which charged Hendricks with one count of conspiracy to provide material support to a foreign terrorist organization and one count of attempting to provide material support to a foreign terrorist organization, both in violation of 18 U.S.C. § 2339B(a)(1). (*See* Doc. 25).

[CLASSIFIED MATERIAL REDACTED].

On October 6, 2016, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Hendricks and this Court that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained or derived from electronic surveillance and physical searches conducted pursuant to [FISA]." (*See* Doc. 20). On July 28, 2017, Hendricks filed his motion. (*See* Doc. 40).

[CLASSIFIED MATERIAL REDACTED].[6]

In subsequent sections of this Memorandum, the Government will: (1) present an overview of the FISA authorities at issue in this case; (2) discuss the FISA process; (3) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; (4) summarize the facts supporting the FISC's probable cause determinations with respect to the target of the electronic surveillance and physical search and to the facility(ies) targeted (all of which information is contained fully in the exhibits in the Sealed Appendix); (5)

[6] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

discuss the relevant minimization procedures; and (6) address the defendant's arguments in support of his motion. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendant's motion, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera*, *ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval; (3) deny the defendant's request that the FISA information be suppressed; and (4) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal.

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED MATERIAL REDACTED].

1. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

2. The FISC's Findings

[CLASSIFIED MATERIAL REDACTED].

II. THE FISA PROCESS

A. OVERVIEW OF FISA[7]

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in

[7] This Memorandum references the statutory language in effect at the time relevant to this matter.

FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISA Ct. Rev."), which is composed of three United States District or Circuit Court Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[8] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General:

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance [or physical search] can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than seven days after the Attorney General authorizes such electronic surveillance [or physical search].

[8] Pub. L. No. 107-56, 115 Stat. 272 (2001).

50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[9] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).[10]

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance and/or physical search within the United States where a significant purpose is the collection of foreign intelligence information.[11] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, foreign intelligence information is defined as:

> (1) information that relates to, and if concerning a United States person[12] is necessary to, the ability of the United States to protect against–
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

---

[9] **[CLASSIFIED MATERIAL REDACTED].**

[10] If no FISC order authorizing the electronic surveillance or physical search is issued, emergency surveillance or search must terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. 50 U.S.C. §§ 1805(e)(3), 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice, notice of the fact of the application, the period of the surveillance, and the fact that during the period information was or was not obtained. 50 U.S.C. §§ 1806(j), 1824(j)(1). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person's consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

[11] **[CLASSIFIED MATERIAL REDACTED].**

[12] **[CLASSIFIED MATERIAL REDACTED].**

> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also* 50 U.S.C. § 1821(1) (adopting the definitions from 50 U.S.C. § 1801). With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;
>
> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures to be followed;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;

> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that the "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. §§ 1823(a)(1)-(8), (a)(3)(B), (C).

1. <u>The Certification</u>

An application to the FISC for a FISA order must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also* 50 U.S.C. § 1823(a)(6).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1) (electronic surveillance), 1821(4)(A) (physical search).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED].

3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance and/or physical search before they are presented to the FISC.

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance and/or physical search only upon finding, among other things, that:

(1) the application has been made by a "Federal officer" and has been approved by the Attorney General;

(2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the statutory requirements set forth in section 1801(h) (electronic surveillance) and section 1821(4) (physical search);

(4) the application contains all of the statements and certifications required by section 1804 (electronic surveillance) or section 1823 (physical search); and

(5) if the target is a United States person, the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean –

(1) a foreign government or any component, thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a)(1)-(7); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. § 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, such activities may be considered by the FISC if there is other activity indicating that the target is an agent of a foreign power. *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999); *United States v. Rosen*, 447 F. Supp. 2d 538, 548-49 (E.D. Va. 2006). The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *See United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008) (finding that the FISA information was lawfully collected and finding specifically, *inter alia*, that "[e]ach application contained facts establishing probable cause to believe that, at the time the application was submitted to the FISC, the target of the FISA collection was an agent of a foreign power . . . ."), *aff'd*, 630 F.3d 102, 129 (2d Cir. 2010); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir.

2000) (concluding that the FISA applications established "probable cause to believe that . . . [the targets] were agents of a foreign power at the time the applications were granted); *Global Relief Found. Inc. v. O'Neill*, 207 F. Supp. 2d 779, 790 (N.D. Ill. 2002) (concluding that "the FISA application established probable cause . . . at the time the search was conducted and the application was granted"), *aff'd* 315 F.3d 748 (7th Cir. 2002). However, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance and/or physical search requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

> (1) the identity, if known, or a description of the specific target of the collection;
> (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
>
> (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;
>
> (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;
>
> (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and
>
> (6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1), (2)(A), 1824(c)(1), (2)(A).

Under FISA, electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and those targeting a non-United States person may be approved for up to 120 days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and one targeting a non-United States person may be approved for up to one year.[13] 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURTS' REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). Under Section 1806(c), the government's notice obligation applies only if the government "intends to enter into evidence or otherwise use or disclose" (2) against an "aggrieved person" [14] (3) in a "trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. § 1806(c); *see also* 50

---

[13] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

[14] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2).

U.S.C. § 1825(d). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the FISA information on two grounds:[15] (1) the information was unlawfully acquired; or (2) the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance or physical search, *i.e.*, the FISA materials. 50 U.S.C. §§ 1806(f), 1825(g). When a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g.*, *United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance and physical search, the district court:

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted.[16]

---

[15] **[CLASSIFIED MATERIAL REDACTED].**

[16] **[CLASSIFIED MATERIAL REDACTED].**

50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General's affidavit or declaration, such as has been filed here, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. §§ 1806(f), 1825(g). Thus, the propriety of the disclosure of any FISA application or order to a defendant may not even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See United States v. Amawi,* 695 F. 3d 457, 474 (6th Cir. 2012) (noting district court's "*in camera* review of the FISA materials"); *Abu-Jihaad*, 630 F.3d at 129 (concluding that "disclosure of FISA materials 'is the exception and *ex parte, in camera* determination is the rule'") (quoting *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009)); *El-Mezain*, 664 F.3d at 565 (quoting 50 U.S.C. § 1806(f)); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982).

If the district court is able to make an accurate determination of the legality of the electronic surveillance and/or physical search based on its *in camera, ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *See Abu-Jihaad,* 630 F.3d at 129 (quoting 50 U.S.C. § 1806(g)); *El-Mezain*, 664 F.3d at 566.

1. *In Camera, Ex Parte* Review Is The Rule

Federal courts have repeatedly and consistently held that FISA anticipates an *ex parte, in camera* determination is to be the rule, with disclosure and an adversarial hearing being the

exception, occurring only when necessary. *See United States v. Amawi,* 531 F. Supp. 2d 832, 837 (N.D. Ohio 2008) ("Where on the basis of what it receives from the government *in camera* and under seal, a district court concludes that it can determine whether a FISA surveillance and search was lawful, it may not order disclosure of any of the FISA materials."); *see also United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1989) (quoting *Belfield*, 692 F.2d at 147); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (quoting *Belfield*, 692 F.2d at 147);[17] *United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) (citing *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991); *El-Mezain*, 664 F.3d at 567 ("[D]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule") (citing *Abu-Jihaad*, 630 F.3d at 129).

In fact, every court but one (whose decision was subsequently overturned by an appellate court)[18] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See, e.g.*, *Omar*, 786 F.3d at 1110-11; *Isa*, 923 F.2d at 1306 ("study of the materials leaves no doubt that substantial national security interests required the *in*

---

[17] In *Duggan*, the Second Circuit explained that disclosure might be necessary if the judge's initial review revealed potential irregularities such as "possible misrepresentations of fact, vague identification of persons to be surveilled or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order." 743 F.2d at 78 (quoting S. Rep. 95-604, at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

[18] In *United States v. Daoud*, the district court ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials to the defense. No. 12 Cr 723, 2014 WL 321384, at *8 (N.D. Ill. Jan. 29, 2014). The Government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose FISA materials, stating, "[s]o clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *United States v. Daoud*, 755 F.3d 479, 485 (7th Cir. 2014).

camera, *ex parte* review, and that the district court properly conducted such a review"); *El-Mezain*, 664 F.3d at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *Stewart*, 590 F.3d at 126-28; *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury (In re Grand Jury Proceedings)*, 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court at the time had ordered disclosure of FISA materials); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *United States v. Kashmiri*, No. 09-CR-830-4, 2010 WL 4705159 at *2-3 (N.D. Ill. Nov. 10, 2010); *United States v. Gowadia*, No. 05-00486, 2009 WL 1649714, at *2 (D. Haw. June 8, 2009); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. Jan. 24, 2008), *aff'd*, 630 F.3d at 129-30; *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130 (D. Mass. Nov. 5, 2007); *United States v. Hassoun*, 04-60001-CR, 2007 WL 1068127, at *4 (S.D. Fla. Apr. 4, 2007); *United States v. Jayyousi*, No. 04-60001, 2007 WL 851278, at *7-8 (S.D. Fla. Mar. 15, 2007), *aff'd*, 657 F.3d 1085 (11th Cir. 2011);[19] *Rosen*, 447 F. Supp. 2d at 546; *United States v. Sattar*, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. Feb. 14, 1997)) (noting "this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance"); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. Oct. 24, 1990); *United States v. Spanjol*, 720 F. Supp. 55, 58-59 (E.D. Pa 1989).

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the FISA-authorized electronic surveillance and physical search in this case that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized

[19] All citations to *Jayyousi* herein are to the Magistrate Judge's Report and Recommendation, which was adopted and incorporated into the Court's Opinion.

and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500, at *14 (E.D.N.Y. Feb. 18, 2016) (finding the review of the FISA materials was "relatively straightforward and not complex" such that the court "was able to evaluate the legality of the challenged surveillance without concluding that due process first warranted disclosure") (internal quotations and citations omitted); *Warsame*, 547 F. Supp. 2d at 987 (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *Thomson*, 752 F. Supp. at 79. This Court, much like the aforementioned courts, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of an Assistant Director of the FBI in support of the Attorney General's Declaration and Claim of Privilege, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *United States v. Ott*, 637 F. Supp. 62, 65 (E.D. Cal. 1986), *aff'd*, 827 F.2d 473 (9th Cir. 1987); *accord Isa*, 923 F.2d at 1306 (the Court's "study of the materials leaves no doubt that substantial

national security interests required the *in camera, ex parte* review, and that the district court properly conducted such a review"); *United States v. Medunjanin*, No. 10-CR-19-1, 2012 WL 526428, at *9 (S.D.N.Y. Feb. 16, 2012) (finding persuasive the Government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation").

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information. . . ." *Central Intelligence Agency v. Sims*, 471 U.S. 159, 175 (1985). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, if revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. Central Intelligence Agency*, 629 F.2d 144, 150 (D.C. Cir. 1980) (noting that "each individual piece of intelligence information, much like a piece of a jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in

itself"); *Medunjanin*, 2012 WL 526428, at *10 (quoting *Yunis*, 867 F.2d at 625). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also ACLU Found. of So. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that Section 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance"); *Stewart*, 590 F.3d at 128 (quoting *Duggan*, 743 F.2d at 77) ("FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security. The applications are required to set forth how and why the Executive Branch knows what it knows, which may include references to covert agents and informers. For this reason, *ex parte*, *in camera* determination is to be the rule").

2. *In Camera, Ex Parte* Review Is Constitutional

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every federal court that has considered the matter, including the Sixth Circuit. *See Damrah*, 412 F.3d 618 at 624 ("FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process"); *see also Abu-Jihaad*, 630 F.3d at 129 (affirming district court's determination that "its *in camera, ex parte* review

permitted it to assess the legality of the challenged surveillance and the requirements of due process did not counsel otherwise"); *Stewart*, 590 F.3d at 126 (noting that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information." (quoting *Duggan*, 743 F. 2d at 73)); *United States v. Fishenko*, No. 12 Civ. 626 (SJ), 2014 WL 8404215, at *7 (E.D.N.Y. Sept. 25, 2014) (citing numerous decisions and concluding that "there is no question as to the constitutionality of FISA"); *El-Mezain*, 664 F.3d at 567 (agreeing with district court that its *in camera, ex parte* review ensured the defendant's constitutional and statutory rights were not violated); *Barr*, 952 F.2d at 465 (procedure under FISA "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance" (citing *Belfield*, 692 F.2d at 141)); *Ott*, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process).

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. *In camera, ex parte* review is the rule in such cases, and that procedure is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate method to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Standard of Review of Probable Cause

In evaluating the legality of the FISA collection, a district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(a), (f), 1825(a), (g).

Although federal courts are not in agreement as to whether the FISC's probable cause determination should be reviewed *de novo* or accorded due deference, the material under review here satisfies either standard of review. *See United States v. Gartenlaub*, 8:14-CR-00173-CAS, Doc. No. 114, at 8 (C.D. Cal. Aug. 6, 2015) ("[T]he Court finds that the materials that it has reviewed *in camera, ex parte* satisfy either standard."); *see also Omar*, slip op. at 12 (2015 WL 3393825 at *7) ("[W]e have no hesitation concluding that probable cause under FISA existed under any standard of review."); *Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review"). The Government respectfully submits that it is appropriate to accord due deference to the findings of the FISC, but notes that a number of courts (including a district court in the Sixth Circuit) have also reviewed the FISC's probable cause determination *de novo*.[20] While in the minority, other courts have afforded due deference to the findings of the FISC. *Abu-Jihaad*, 630 F.3d at 130; *accord United States v. Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007,

[20] **[CLASSIFIED MATERIAL REDACTED].**

at *21-22 (N.D. Ga. Mar. 19, 2009) (FISC's "determination of probable cause should be given 'great deference' by the reviewing court") (citing *Illinois v. Gates*, 462 U.S. at 236).

In the analogous area of criminal searches and surveillance, the law in the Sixth Circuit, as well as that in other federal circuits, accords great deference to a magistrate judge's probable cause determinations. *See, e.g.*, *United States v. Allen*, 211 F.3d 970, 973 (6th Cir. 2000); *see also United States v. Krupa*, 658 F.3d 1174, 1177 (9th Cir. 2011); *United States v. Smith*, 581 F.3d 692, 694 (8th Cir. 2009); *United States v. Joseph*, 709 F.3d 1082, 1093 (11th Cir. 2013) (citing *Illinois v. Gates*, 462 U.S. at 236); *United States v. Robinson*, 724 F.3d 878, 884 (7th Cir. 2013). It would thus be consistent for a court that is reviewing FISA-authorized electronic surveillance and physical search to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure. *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (according the same deference to the FISC's probable cause determination as to a magistrate's criminal probable cause determination); *cf. United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause).[21]

2. Probable Cause Standard

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about

[21] *Ahmed* is not alone in analogizing FISA orders to search warrants. *See, e.g.*, *In re Sealed Case*, 310 F.3d 717, 774 (FISA Ct. Rev. 2002) (declining to decide whether a FISA order constitutes a warrant, but noting "that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment"); *but see Warsame*, 547 F. Supp. 2d at 992 n.10 (noting that the need for foreign intelligence justifies an exception to the warrant requirement).

to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a), 1824(a); *United States v. Alwan*, No. 1:11-CR-13, 2012 WL 399154, at *8-10 (W.D. Ky. Feb. 7, 2012); *Abu-Jihaad*, 630 F.3d at 130. It is this standard – not the standard applicable to criminal search warrants – that this Court must apply. *See Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power.") (quoting *El-Mezain*, 664 F.3d at 564); *Duka*, 671 F.3d at 338; *El-Mezain*, 664 F.3d at 564; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court (Keith I)*, 407 U.S. 297, 322 (1972) and (*United States v. U.S. Dist. Court for the E. Dist. of Mich., S. Div.* (*Keith II*), 407 U.S. 297, 322 (1972)); *Medunjanin*, 2012 WL 526428, at *6 ("[N]o branch of government – whether executive or judicial – need make a probable cause finding of *actual or potential* criminal activity to justify a FISA warrant").

The probable cause showing the Government must satisfy before receiving authorization to conduct electronic surveillance or physical search under FISA complies with the Fourth Amendment's reasonableness standard. The argument that FISA's different probable cause standard violates the Fourth Amendment's reasonableness requirement has been uniformly rejected by federal courts. *See, e.g.*, *Damrah*, 412 F.3d at 625 ("FISA has uniformly held to be consistent with the Fourth Amendment"); *Abu-Jihaad*, 630 F.3d at 120 (rejecting the defendant's Fourth Amendment claim and listing 16 cases that stand for the proposition that FISA does not violate the Fourth Amendment).

[CLASSIFIED MATERIAL REDACTED].

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008) (quoting *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987)); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011); *Warsame*, 547 F. Supp. 2d at 990. When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. A district court's review should determine whether the certifications were made in accordance with FISA's requirements. Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.*; *Rahman*, 861 F. Supp. at 250 (citing *Duggan*); *United States v. Omar*, No. CR-09-242, 2012 WL 2357734, at *3 (D. Minn. June 20, 2012) ("The reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' . . . absent a showing sufficient to trigger a *Franks* hearing." (quoting *Duggan*, 743 F. 2d at 77)); *In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Kashmiri*, 2010 WL 4705159, at *1; *United States v. Islamic Am. Relief Agency* (*IARA*), No. 07-87-Cr-NKL), 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009). When the target is a United States person, the district court should also ensure that each certification is not "clearly erroneous." *Duggan*, 743 F.2d at 77; *Campa*, 529 F.3d at 994; *Kashmiri*, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established only when "the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S.*

Gypsum Co., 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005) (quoting *U.S. Gypsum Co.*, 333 U.S. at 395).

4. FISA Is Subject to the "Good Faith" Exception

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not met, the evidence obtained or derived from the FISA-authorized electronic surveillance and physical search is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 (noting that federal officers are entitled to rely in good faith on a FISA warrant (citing *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007))).

The FISA-authorized electronic surveillance and physical search at issue in this case, authorized by a duly enacted statute and an order issued by a neutral judicial officer, would fall squarely within this good faith exception. There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the electronic surveillance and physical search at issue. *See Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to that order would be admissible under *Leon*'s good faith exception to the exclusionary rule.

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED].

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED].

1. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

2. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

a. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

b. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

c. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

d. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

e. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

f. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

3. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED].[22]

1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED].

2. "A Significant Purpose"

[CLASSIFIED MATERIAL REDACTED].

2. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED].

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN COMFORMITY WITH AN ORDER OF AUTHORIZATION OF APPROVAL

[CLASSIFIED MATERIAL REDACTED].

1. The Minimization Procedures

Once a reviewing court is satisfied that the FISA information was lawfully acquired, it must then examine whether the electronic surveillance and physical search were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical search were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED].

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into

[22] The defendant concedes that the "clearly erroneous" standard is the appropriate standard to be applied to the Court's review of the required certifications. (Doc. 40 at 11).

account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741. Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]innocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. 1, at 55 (1978)); *see also United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004), *rev'd on other grounds;* 543 U.S. 1097 (2005), *op. reinstated in pertinent part;* 405 F.3d 1034 (4th Cir. 2005) (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000). One court recognized that "the Congress that enacted FISA observed that 'bits and pieces of information, which taken separately could not possibly be considered "necessary" may together over time take on significance.'" *Medunjanin*, 2012 WL 526428, at *4 (quoting H.R. Rep. No. 95-1283,

pt. 1, at 58-59). As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, at least one court has cautioned that, when a United States person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. Accordingly, to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Id.* at 81-82 (quoting H.R. Rep. No. 1283, pt. 1, at 59).

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39

(1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008 (quoting *United States v. Bynum,* 485 F.2d 490, 500 (2d Cir. 1973)). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334; *see also United States v. Goffer*, 756 F. Supp. 2d 588, 592 (S.D.N.Y. 2011) (referencing Title III wiretap surveillance).

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135 (D. Mass. 2007); *see also Hammoud*, 381 F.3d at 334 ("The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information." (citing S. Rep. No. 95-701, at 39-40 (1978))); *Hasbajrami*, 2016 WL 1029500, at *14 (quoting *Mubayyid*); *Sattar*, 2003 WL 22137012, at *10-11; S. Rep. No. 95-701, at 39-40, 1978 U.S.C.C.A.N., at 4008-09 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion").

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that

"[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See id.* at 1305.

Assuming, for the sake of argument, that certain communications were not minimized in accordance with the SMPs, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

H.R. Rep. No. 1283, pt. 1, at 93; *see also Falcone*, 364 F. Supp. at 886-87; *Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED].

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collection discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collection discussed herein was lawfully conducted under the

minimization procedures approved by the FISC and applicable to the FISA collection discussed herein.

V. THE COURT SHOULD REJECT THE DEFENDANT'S LEGAL ARGUMENTS

The defendant's motion seeks the following: (1) suppression of the FISA information and (2) disclosure of the FISA materials. (*See* Doc. 40). For the reasons set forth below and as the Court will see in its *ex parte*, *in camera* review of the FISA materials, the defendant's arguments are without merit.

A. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION

[CLASSIFIED MATERIAL REDACTED].

1. "Raw Intelligence" Is Not Inherently Unreliable

The defendant suggests that the FISA application(s) may have contained "raw intelligence," which may not have been "reliable and/or had a verifiable track record, or was [not] independently corroborated." (Doc. 40 at 11). The defendant does not define "raw intelligence" and does not cite any cases to support his position. In fact, courts that have addressed the issue of raw intelligence have made it clear that it is not inherently unreliable. *Alsabri v. Obama*, 764 F. Supp. 2d 60, 91 (D.D.C. 2011). In *Barhoumi v. Obama* , the D.C. Circuit found no basis for "a per se rule that information contained in an intelligence report is inherently unreliable." 609 F.3d 416, 429 (D.C. Cir. 2010). To the contrary, such information need only "be presented in a form, or with sufficient additional information, that permits . . . [the] court to assess its reliability." *Id.* (quoting *Parhat v. Gates*, 532 F.3d 834, 847, 849 (D.C. Cir. 2008)) ("[W]e do not suggest that hearsay evidence is never reliable."). The same is true in the more analogous context of criminal search warrants. In making probable cause determinations based on a totality of the circumstances, courts routinely review information

presented in search warrant affidavits for indicia of reliability or independent corroboration. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983) (probable cause sufficient, based on totality of the circumstances, where anonymous informant's recitation of detailed facts was corroborated by police observation); *Draper v. United States*, 358 U.S. 307, 313 (1959) (probable cause sufficient where hearsay information from previously reliable source was corroborated by independent police investigation); *United States v. Martinez-Garcia*, 397 F.3d 1205, 1216-17 (9th Cir. 2005) (probable cause sufficient where reliable informant told police he had purchased drugs from defendant, and police observed three controlled drug buys).

[CLASSIFIED MATERIAL REDACTED].

2. <u>The Government Satisfied the Probable Cause Requirements of FISA</u>

The defendant asserts that there was no probable cause to believe that he was an agent of a foreign power. (Doc. 40 at 9-14). Probable cause, while more than a bare suspicion, is "less than absolute certainty," and in making the probable cause determination, FISA permits a judge to "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." *Rosen*, 477 F.Supp. 2d at 549 (quoting *Illinois v. Gates*, 462 U.S. at 238); 50 U.S.C. § 1805(b). Furthermore, the FISA probable cause standard "does not necessarily require a showing of an imminent violation of criminal law" because Congress clearly intended a different showing of probable cause for these activities than that applicable to ordinary cases.[23] *Rosen*, 477 F.Supp. 2d at 549 (citing *In re Sealed Case*, 310 F.3d. at 739); *see also United States v. Osmakac*, No. 8:12-CR-00045, 2017 WL 3574600, at *11 (11th Cir. 2017). Here, a review of the FISA materials shows that the Government plainly satisfied the requirements of FISA.

---

[23] **[CLASSIFIED MATERIAL REDACTED].**

[CLASSIFIED MATERIAL REDACTED].

The defendant also claims that the Government's probable cause showing may have been based solely on his "expressive behavior" during "online activities" with "unindicted co-conspirators," which is activity protected by the First Amendment. (Doc. 40 at 13). Contrary to the defendant's claim, not all speech- or advocacy-related activities fall within the protection of the First Amendment. For instance, conversations with co-conspirators merit no First Amendment protection because they are statements made in furtherance of a conspiracy and are evidence of the participant's criminal intent. "Numerous crimes under the federal criminal code are, or can be, committed by speech alone . . . . [I]f the evidence shows that the speech crossed the line into criminal solicitation, procurement of criminal activity, or conspiracy to violate the laws, the prosecution is permissible." *United States v. Rahman*, 189 F.3d 88, 117 (2d Cir. 2008); *United States v. Sattar*, 395 F. Supp. 2d 79, 101 (S.D.N.Y. 2005) ("First Amendment lends no protection to participation in conspiracy, even if such participation is through speech").

[CLASSIFIED MATERIAL REDACTED].

3. <u>The Certification(s) Complied with FISA</u>

The defendant also claims that there may be defects in the certification(s) included in the FISA application(s). Specifically, the defendant argues that the application(s) fail to demonstrate that the gathering of foreign intelligence information was a "significant purpose" of the FISA order(s). (Doc. 40 at 17). Additionally, the defendant argues that certifying that the information could not have been obtained through normal investigative techniques was incorrect. (Doc. 40 at 17-18). Furthermore, the defendant suggests that this Court "should carefully examine the dates" in the certification(s) to determine whether the duration of the FISC-authorized collection was proper. (Doc. 40 at 18).

[CLASSIFIED MATERIAL REDACTED].

4. The Government Complied with the Minimization Procedures

[CLASSIFIED MATERIAL REDACTED].

The Government respectfully submits that the Court's *ex parte*, *in camera* review of the FISA materials will demonstrate that the Government complied with all of FISA's statutory requirements. Accordingly, the Government submits that there is no basis to suppress the FISA information in the present case.

5. FISA's Significant Purpose Standard Is Constitutional[24]

[CLASSIFIED MATERIAL REDACTED].[25]

As the Third Circuit noted in *Duka*, the "significant purpose" standard "reflects a balance struck by Congress . . . to promote coordination between intelligence and law enforcement officials in combating terrorism, acknowledging that, as a practical matter, these functions inevitably overlap." *Duka*, 671 F.3d at 343. The *Duka* Court noted that *Keith*, 407 U.S. at 322-23, required Congress's judgment be accorded "some additional measure of deference" by the

---

[24] To the extent the defendant challenges the procedures dictated by Title I and III of FISA as they relate to the Fourth Amendment, the courts have uniformly found FISA to be consistent with the Fourth Amendment. *See Damrah*, 412 F.3d at 625 (citing *e.g., In re Sealed Case*, 310 F.3d 717, 742-47 (FISA Ct. Rev. 2002)); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *Cavanagh*, 807 F.2d at 790-92; *Duggan*, 743 F.2d at 73 n.5; *See also Abu-Jihaad*, 630 F.3d at 120 (rejecting the defendant's Fourth Amendment claim and listing 16 cases that stand for the proposition that FISA does not violate the Fourth Amendment).

[25] The defendant's reliance on *Mayfield v. United States,* 504 F. Supp. 2d 1023 (D. Or. 2007) to challenge the constitutionality of FISA's "significant purpose" test on Fourth Amendment grounds is misplaced. (*See* Doc. 61, at 13-15). FISA's "significant purpose" standard was held unconstitutional in *Mayfield*, a civil case, which the Ninth Circuit eventually vacated on the ground that the plaintiff lacked standing. *See Mayfield v. United States*, 599 F.3d 964, 973 (9th Cir. 2010). When a judgment is vacated by a higher court, "it deprives the [lower] court's opinion of precedential effect." *Los Angeles County v. Davis*, 440 U.S. 625, 634 n. 6 (1979). Moreover, the district court's rationale in *Mayfield* was specifically rejected in *Kashmiri*, 2010 WL 4705159, at * 8.

courts, adding "even leaving Congress's judgment aside, we conclude that FISA's 'significant purpose' standard is reasonable in light of the government's legitimate national security goals." *Id.*

Moreover, the fact that criminal prosecution is one of the possible purposes is not fatal.[26] *See Abu-Jihaad*, 630 F.3d at 128-29; *In re Sealed Case,* 310 F.3d at 735. Even under the "primary purpose" standard, courts "refuse[d] to draw too fine a distinction between criminal and intelligence investigations." *Sarkissian*, 841 F.2d at 965. According to one Court, the fact that "the government may later choose to prosecute is irrelevant," as "FISA contemplates prosecution based on evidence gathered through surveillance" to secure foreign intelligence information. *Id.* The *Abu-Jihaad* court rejected the argument that FISA is unconstitutional because it does not require certification of a primary purpose to obtain foreign intelligence information and stated:

> We conclude that FISA's significant purpose requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering . . . *The fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion.* We reject the argument that FISA is unconstitutional because it does not require certification of a primary purpose to obtain foreign intelligence information.

Id. at 128-29 (emphasis added). For these reasons, the defendant's argument fails and this Court should deny his Motion to Suppress.

6. ***Franks v. Delaware*** **Does Not Require an Evidentiary Hearing Regarding the Suppression of the FISA Materials**

Moreover, the defendant speculates that there were "intentional or reckless" omissions in the application(s) submitted to the FISC, in violation of *Franks v. Delaware*, 438 U.S. 154 (1978), and seeks an evidentiary hearing relating to the disclosure of the FISA materials based on

[26] A criminal prosecution motive is only fatal if the Court finds the Government's significant purpose certification in the FISA application is clearly erroneous. *See Abu-Jihaad,* 630 F.3d at 128.

this speculation. (*See* Doc. 40 at 14-17). Based on the relevant case law, this Court should decline to hold such a hearing. To merit a *Franks* hearing, a defendant must make a "concrete and substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56. Courts apply the same standard when a defendant seeks a *Franks* hearing as part of a challenge to FISA collection; to obtain a hearing, a defendant must "make 'a substantial preliminary showing that a false statement knowingly or intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application." *Duggan*, 743 F.2d at 77 n.6 (quoting *Franks*, 438 U.S. at 155-56). A defendant must show that the agent lied or recklessly disregarded the truth with specific evidence in the form of "[a]ffidavits or sworn or otherwise reliable statements of witnesses." *Franks*, 438 U.S. at 171. The *Franks* threshold is not met even by an offer of proof of an impropriety that might have affected the outcome of the probable cause determination, but rather requires one that was "necessary to the finding of probable cause." *United States v. Colkley*, 899 F.2d 297, 301-02 (4th Cir. 1990); *see also United States v. Shnewer*, No. 07-459, 2008 U.S. Dist. LEXIS 112001, at *38 (D.N.J. Dec. 29, 2009) ("[E]ven if the Court were to determine there existed a reckless or intentional falsehood or omission in the FISA application materials, the evidence obtained still should not be suppressed unless the Court makes the further finding that the falsehood or omission was material to the probable cause determination.").[27]

[27] *See Alwan*, 2012 WL 399154, at *8-10, ("The Court is cognizant of the substantial difficulties [the defendant] has encountered in trying to assert a *Franks* violation. Regardless of the difficulties, however, it does not change the evidentiary burden he must meet.")

Only after a defendant makes the requisite showing may the Court conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, in the FISA applications sufficient to warrant suppression of the FISA-obtained or -derived evidence.[28] *Franks*, 438 U.S. at 171. The defendant, however, ignores this burden and instead cites the "possibility" that such misstatements or omissions exist, based on reports of misstatements and omissions in at least 75 other FISA applications in the years 2000 through 2001 and a Department of Justice (DOJ) report related to "over collection" in 2005. (Doc. 40 at 15-16). Citing prior instances of purported government misrepresentations or omissions in other, unrelated cases, however, cannot satisfy the *Franks* standard, "as it sheds no light on the truth or falsity of the particular FISA application under review." *Daoud*, 755 F.3d at 492 (Rovner, J. concurring); *see also Warsame*, 547 F. Supp. 2d at 987-88 (stating that defense allegations that "the government has included misstatements and critical omissions in other FISA applications not at issue here cannot justify disclosure in this case").

In fact, an argument identical to Hendricks' was presented to the court in *United States v. Aziz*, 228 F. Supp. 3d 363, 371-372 (M.D. Pa. 2017), and was rejected. In part, the *Aziz* court held:

> There is no indication that these errors have persisted. To the contrary, the FISC noted that the Federal Bureau of Investigation thereafter 'promulgated detailed procedures governing the submission of requests to conduct FISA surveillance and searches' in an effort to remedy the problem. In any event, the FISC's remarks do not increase the likelihood of a misstatement here. As one court observed: the FISC's appraisal of generalized errors is no more probative of an error in this case 'than a general study of errors

[28] Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held where the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. *Franks*, 438 U.S. at 171; *Colkley*, 899 F.2d at 300; *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

> committed over a period of years in baseball would be probative of whether errors occurred in a specific game.' *Rosen*, 447 F. Supp. 2d at 552.

The Court also noted that the 2006 DOJ report found that "sixty-nine percent (69%) of reported intelligence violations in 2005 . . . raise doubts only as to agency compliance with orders once received they contain no express or implied observations regarding the accuracy of FISA applications themselves." *Id.* As a result, there was "no arguable basis for the court to convene a *Franks* hearing," just as here, where the defendant advances no valid argument for such an adversary hearing on the suppression motion.

Nonetheless, the defendant claims that a *Franks* hearing and disclosure of the FISA materials "is necessary in order to permit [the defendant] the opportunity to prove that the affiants before the FISC intentionally or recklessly made materially false statements and omitted material information from the FISA applications," (Doc. 40 at 17), an approach which would allow Hendricks, and defendants in every case, to obtain the FISA materials by merely alleging some impropriety.[29] Disclosing FISA materials to defendants would then become the rule, violating Congress' clear intention, set forth in 50 U.S.C. §§ 1806(f) and 1825(g), that the FISA materials be reviewed *in camera* and *ex parte* in a manner consistent with the realities of modern intelligence needs and investigative techniques. Courts have acknowledged that the FISA statute does not envision such disclosure without establishing a basis for it. For instance, the *Daoud* court noted that it was "hard" for a defendant to make the *Franks* showing "without access to the classified [FISA] materials," but the "drafters of [FISA] devised a solution: the judge makes the initial determination, based on full access to all classified materials. . . ." *Daoud*, 755 F.3d at

[29] One judge referred to this as "backwards reasoning" in denying a defendant's motion to suppress FISA-derived evidence. *United States v. Mihalik*, 11-CR-833(A), Doc. No. 108, at 2 (C.D. Cal. Oct. 3, 2012) (Minute Order Denying Defendant's Motion to Suppress FISA-Derived Evidence).

483-84. Similarly, in *Belfield*, the court noted that "Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure." *Belfield*, 692 F.2d at 148; *see also Kashmiri*, 2010 WL 4705159, at *6.

Courts have rejected other defendants' attempts to force a *Franks* hearing by positing unsupported speculation to challenge the validity of FISC orders, and this Court should do so here. *See Abu-Jihaad*, 531 F. Supp. 2d at 309; *Kashmiri*, 2010 WL 4705159, at *6 (noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review"); *Shnewer*, 2008 U.S. Dist. LEXIS 112001, at *37 ("This catch-22 has not troubled courts, however, and they defer to FISA's statutory scheme."); *Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA — which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards — would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation."); *Hassoun*, 2007 WL 1068127, at *4.

Here, the defendant has failed to carry the burden of establishing the prerequisites for an adversary hearing, and his attempt to obtain disclosure of the FISA materials to meet that burden is unprecedented and runs counter to FISA, *Franks*, and the intent of Congress. For these reasons, the Court should deny the defendant's request for an adversary hearing on his suppression motion. Moreover, the Government respectfully submits that this Court's *in camera*, *ex parte* review of the FISA materials will demonstrate that "an adversary hearing in this case would be academic because there is no question the FISA application [or applications]

passes [or pass] muster." *Medunjanin*, 2012 WL 526428, at *9. Under these circumstances, the defendant's motion should be denied.

B. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR DISCLOSURE OF THE FISA MATERIALS

In support of his argument for disclosure of the FISA materials, the defendant claims that disclosure: (1) "may be 'necessary' under § 1806(f)"; (2) is required under § 1806(g) and due process; (3) is required by the adversary system of justice; and (4) is appropriate because defense counsel may be in the process of obtaining a security clearance. (Doc. 40 at 19-25). For the following reasons, the Court should deny the request for disclosure.

1. Disclosure Is Not "Necessary" under FISA

The defendant asserts that "there are ample justifications for disclosure of the FISA applications, which would permit defense counsel an opportunity to demonstrate that the requisite probable cause was lacking, including specifically, that the information in the applications was unreliable or obtained via illegal means." (Doc. 40 at 20). The defendant is seeking disclosure to bolster his argument for suppression, which is not permissible under the statute.

There is only one reason to disclose the FISA materials to defense counsel. The Court must conduct its review of those materials *in camera* and *ex parte*, and disclosure is within the Court's discretion only following that review and only if the Court is unable to determine the legality of the electronic surveillance and/or physical search without the assistance of defense counsel. 50 U.S.C. §§ 1806(f), 1825(g); *Daoud*, 755 F.3d at 482; *Rosen*, 447 F. Supp. 2d at 546; *Duggan*, 743 F.2d at 78. This holding is fully supported by the legislative history of 50 U.S.C. § 1806(f), which states: "The court may order disclosure to [the defense] only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . .

Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied." S. Rep. No. 95-701, 95th Cong., 2d Sess., 64-65 (1978) (Senate Report); *see also United States v. Hassan*, 742 F.3d 104, 138 (4th Cir. 2014) (where the court "emphasized that, where the documents 'submitted by the government [are] sufficient' to 'determine the legality of the surveillance,' the FISA materials should not be disclosed.") (quoting *Squillacote*, 221 F.3d at 554). As this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that will allow the Court to make its determination of the lawfulness of the FISA collection without input from defense counsel.

The defendant's request, which effectively calls for disclosure where defense counsel could provide assistance, instead of where necessary, is merely an attempt to circumvent the clear language of the statute. *See* 50 U.S.C. §§ 1806(f), 1825(g). As the *Belfield* court stated, "Congress was adamant, in enacting FISA, that [its] 'carefully drawn procedure[s]' are not to be bypassed." 692 F.2d at 146 (citing Senate Report at 63); *see also United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *32 (D. Or. June 24, 2014) ("Obviously it would be helpful to the court to have defense counsel review the materials prior to making arguments. Congress, however, did not put 'helpful' in the statute; it chose 'necessary.'"), *aff'd*, No. 14-30217, 2016 WL 7046751 (9th Cir. Dec. 5, 2016). As the *Daoud* Court stated, "the defendant's misreading of the statute" would circumvent the required *in camera, ex parte* review whenever a defense counsel "believed disclosure necessary, since if the judge does not conduct the *ex parte* review, she will have no basis for doubting the lawyer's claim of necessity." 755 F.3d at 482.

The defendant is not entitled to the FISA materials for the purpose of challenging the lawfulness of the FISA authorities, as FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the court

noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428, at *10; *see also Badia*, 827 F.2d at 1464 (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors"); *Mubayyid*, 521 F. Supp. 2d at 131.

The defendant has failed to present any colorable basis for disclosure, as this Court is able to review and make a determination as to the legality of the FISA collection without the assistance of defense counsel. Where, as here, defense participation is not necessary, FISA requires that the FISA materials remain protected from disclosure. Congress's clear intention is that FISA materials should be reviewed *in camera* and *ex parte* and in a manner consistent with the realities of modern intelligence needs and investigative techniques. There is simply nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials. *See Rosen*, 447 F. Supp. 2d at 546 (stating that "exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively" (citing *Belfield*, 692 F.2d at 147).

2. Due Process Does Not Require Disclosure

The defendant also claims that he is entitled to disclosure of the FISA materials under 50 U.S.C. § 1806(g) and the Due Process Clause of the Fifth Amendment. (Doc. 40 at 21). Courts are in agreement, however, that FISA's *in camera*, *ex parte* review does not violate due process, nor does due process require that defendants be granted access to the FISA materials except as provided for in 50 U.S.C. §§ 1806(f), (g) and 1825(g), (h). *See, e.g.*, *El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 117; *Damrah*, 412 F.3d at 624; *Ott*, 827 F.2d at 476-77; *Belfield*, 692

F.2d at 148-49; *Nicholson*, 2010 WL 1641167, at *3-4; *Gowadia*, 2009 WL 1649714, at *2; *Jayyousi*, 2007 WL 851278, at *7-8; *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); *ACLU Foundation*, 952 F.2d at 465; *Nicholson*, 955 F. Supp. at 592 (finding, based on "the unanimous holdings of prior case law, . . . that FISA does not violate the Fifth or Sixth Amendment by authorizing *ex parte in camera* review."); *Spanjol*, 720 F. Supp. at 58-59; *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. 1983); *United States v. Falvey*, 540 F. Supp. 1306, 1315-1316 (E.D.N.Y. 1982).

The plain intention of 50 U.S.C. §§ 1806(g) and §1825(h) — allowing the Court to order disclosure of material to which the defendant would be entitled under the Due Process Clause, such as material that had not been previously disclosed under *Brady*, even while ruling against the defendant's motion generally — cannot be interpreted to support the defendant's demand for access to all of the FISA materials in advance of the Court's *in camera, ex parte* review and determination of the legality of the collection. *See Amawi*, 695 F. 3d at 475 (rejecting defendant's due process argument and upholding the district court's decision not to disclose FISA materials to the defense under *Brady*). With respect to any claim that the FISA materials contain information that due process requires be disclosed to the defense, the request is premature since the Court will make that factual determination for itself during its *in camera, ex parte* review. The Government is confident that the Court's review of the challenged FISA materials will not reveal any additional material that due process requires be disclosed to the defendant, such as *Brady* material, as provided for in 50 U.S.C. §§ 1806(g) and 1825(h). *See Amawi*, 531 F. Supp. 2d at 837. Accordingly, the defendant's claim that he is entitled to the disclosure of the FISA materials under 50 U.S.C. §§ 1806(g) and 1825(h), and due process should be rejected.

3. The Adversary System Does Not Require Disclosure

Furthermore, the defendant claims that he is entitled to disclosure because the lack thereof "would render the proceedings . . . *ex parte*," and thus "antithetical to the adversary system that is the hallmark of American criminal justice." (Doc. 40 at 21-24). This claim is contrary to all of the relevant case law (as opposed to the case law cited by the defense, all of which predates FISA or does not address FISA). Several courts have addressed the right to confrontation in this context and found that "FISA's *in camera* review provisions have been held to be constitutional." *Osmakac*, 2017 WL 3574600, at *13-14; *Nicholson*, 2010 WL 1641167, at *3 (citing *Isa*, 923 F.2d at 1307-08 (Sixth Amendment right of confrontation is not violated by FISA's *in camera* review procedure)); *see also United States v. Thomas*, 201 F. Supp. 3d 643 at 648-649 (E.D. Pa. 2016) (rejecting the defendant's "apparent contention that FISA's *ex parte* provisions are *per se* unlawful"); *United States v. Hussein*, No. 13CR1514-JM, 2014 U.S. Dist. LEXIS 59400, at *8 (S.D. Cal. Apr. 29, 2014) (The "*in camera, ex parte* review process under FISA satisfies due process under the United States Constitution."); *United States v. Lahiji*, No. 3:10-506-KF, 2013 WL 550492, at *4 (D. Or. Feb. 12, 2013) (the court found no violation of defendants' Fourth, Fifth, or Sixth Amendment rights); *United States v. Jamal*, No. CV-09-0332-PHX-FSM, 2011 U.S. Dist. LEXIS 12224, at *5 (D. Az. Feb. 7, 2011) (movant's Sixth Amendment rights were not violated by trial counsel's inability to discuss FISA materials); *Benkahla*, 437 F. Supp. 2d at 554; *Nicholson*, 955 F. Supp. at 592 ("Based on the unanimous holdings of prior case law, . . . FISA does not violate . . . the Sixth Amendment by authorizing *ex parte in camera* review."); *Falvey*, 540 F. Supp. at 1315-16 (rejecting First, Fifth, and Sixth Amendment challenges and noting that a "massive body of pre-FISA case law of the Supreme

Court, Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis).

Courts have also consistently rejected similar arguments challenging FISA under the Sixth Amendment. *See Isa*, 923 F.2d at 1306-07; *Belfield*, 692 F.2d at 148; *Lahiji*, 2013 WL 550492, at *4; *Warsame*, 547 F. Supp. 2d at 988 n.4 (finding argument "without merit") (citing *Nicholson*, 955 F. Supp. at 592); *Megahey*, 553 F. Supp. at 1193. In overturning a district court's order to disclose FISA materials to the defense, the *Daoud* Court described the belief that "adversary procedure is always essential to resolve contested issues of fact" as "an incomplete description of the American legal system in general and the federal judicial system in particular." 755 F.3d at 482; *see also Thomas*, 201 F. Supp. 3d at 648-649 (quoting *Daoud*, 755 F.3d at 482).

4. A Security Clearance Does Not Entitle Defense Counsel to the FISA Materials

Finally, the defendant asserts that the fact his counsel is in the process of obtaining a security clearance means the Court should disclose the FISA materials subject to an "appropriate protective order." (Doc. 40 at 20). As discussed above, the only statutory authorities that grant a court discretion to disclose the FISA materials at this stage is set out at 50 U.S.C. §§ 1806(f) and 1825(g), and these provisions permit disclosure only where the court finds that it is unable to determine the legality of the electronic surveillance and physical search based on its *in camera, ex parte* review alone and without the assistance of defense counsel. Defense counsel's security clearance does not affect the need to have an *ex parte, in camera review* to determine whether disclosure would harm national security. *Daoud*, 755 F.3d at 481-486; *see also Abu-Jihaad*, 630 F.3d at 129 (pursuant to FISA a district court must review *in camera* and *ex parte* the FISA materials and may only order disclosure to the extent required by due process).

In the FISA context, courts have consistently held that while holding a valid security clearance is a necessary prerequisite to reviewing classified information, it is not a sufficient basis for a court to order disclosure of classified information to defense counsel. Instead, cleared counsel only has a "need to know" if the Court determining the legality of the surveillance concluded that disclosure is "necessary." In *Bin Laden*, the court denied the disclosure of the FISA materials to cleared counsel, noting that "[d]efense counsel's [*sic*] assertion that, given their security clearances, they ought to have access to the sensitive documents is not persuasive to this Court. As the Government explains, those security clearances enable attorneys to review classified documents, 'but they do not entitle them to see all documents with that classification.'" 126 F. Supp. 2d at 287 n. 27, *aff'd by In re Terrorist Bombings in East Africa*, 552 F.3d 157 (2d Cir. 2008). The Ninth Circuit in *Ott* also rejected this argument, noting Congress's

> legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy a security clearance. We reject the notion that a defendant's due process right to disclosure of FISA materials turns on the qualifications of his counsel.

827 F.2d at 476-77; *see also Nicholson*, 2010 WL 1641167, at *5 (referencing *Ott* and holding that "[b]ased on [the court's] *in-camera* review . . . the disclosure of FISA materials to [cleared] defense counsel is neither required nor appropriate"); *Al-Kidd v. Gonzalez,* 2008 WL 5123009 at *7 (D. Idaho 2008) ("despite plaintiff counsel's security clearances and therefore their ability to review sensitive information, the [*Ott*] court denied the plaintiff access to materials gathered pursuant to FISA. . . . [E]ven with a protective order and appropriate security clearances, this Court may still deny al-Kidd access to the information."); *Warsame*, 547 F.Supp.2d at 989 n.5; *El-Mezain*, 664 F.3d at 568.

Courts have repeatedly held that defense counsel are required to have more than a security clearance — defense counsel must also have a need to know. One court has addressed the "need to know requirement" by stating:

> [i]t's also a mistake to think that simple possession of a security clearance automatically entitles its possessor to access to classified information that he is cleared to see . . . . So in addition to having the requisite clearance the seeker must convince the holder of the information of the seeker's need to know it.

Daoud, 755 F.3d at 484.[30] "A clearance itself" is not enough for access to classified information: there is quite sensibly, also a 'need to know' requirement. . . . Clearance simply qualifies counsel to view secret materials. It does not, however, *entitle* counsel to see anything and everything that the government has stamped classified even if it has something to do with a client." *United States v. Amawi*, 2009 WL 961143, at *1, 2 (N.D. Ohio 2009) (emphasis in original); *see also Medunjanin*, 2012 WL 526428, at *9 ("Defense counsel's security clearances add little to the case for disclosure. . . . As the government persuasively argues, unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation."); *United States v. Libby*, 429 F. Supp. 2d 18, 24 n. 8 (D.D.C. 2008) ("It is axiomatic that even if the defendant and his attorneys had been granted the highest level of security clearances, that fact alone would not entitle them to access to every piece of classified information this country possesses."). If this Court concludes from its *in camera, ex parte* review of the FISA materials that it is capable of accurately determining

[30] As the Seventh Circuit explained in *Daoud*, disclosing state secrets to cleared counsel could in fact harm national security because cleared counsel "might in their zeal to defend their client, to whom they owe a duty of candid communication, or misremembering what is classified and what is not, inadvertently say things that would provide clues to classified material." 755 F.3d at 484. The potential threat that classified information may be disclosed to the defendant, even inadvertently, is further justification for the FISA materials to not be disclosed to cleared defense counsel.

the legality of the FISA collection at issue, then no defense attorney, even one with an otherwise appropriate security clearance, would have a "need to know" any of the FISA materials.

The defendant's arguments in support of disclosure of the FISA materials have no basis in the law, and disclosure of the FISA materials would cause exceptionally grave damage to the national security. The Government respectfully submits that, contrary to the defendant's assertions, there is nothing extraordinary about this case to justify an order to disclose the highly sensitive and classified FISA materials in this case under the applicable FISA standard. *See Amawi*, 531 F. Supp. 2d at 839 ("nothing in those materials comes within the government's *Brady* obligations, or otherwise could properly provide a basis for granting the defendants' motion for disclosure."); *Rosen*, 477 F. Supp. 2d at 546 ("Review of the FISA applications, orders and other materials in this case presented none of the concerns that might warrant disclosure to the defense."). Accordingly, the defendant's motion for disclosure of the FISA materials should be denied.

VI. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION OR DISCLOSE THE FISA MATERIALS

For the foregoing reasons, the defendant's motion should be denied without a hearing. The Attorney General has filed a declaration in this case stating that disclosure of or an adversary hearing with respect to the FISA materials would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera, ex parte* review of the challenged FISA materials to determine whether the information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In conducting that review, the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. §§ 1806(f), 1825(g). Congress, in enacting

FISA's procedures for *in camera, ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. The FISA materials at issue here, which have been submitted for *in camera, ex parte* review in the Sealed Appendix, are organized and readily understood, and an overview of them has been presented herein as a frame of reference. This Court will be able to render a determination based on its *in camera, ex parte* review, and the defendant has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

Furthermore, the Government respectfully submits that the Court's examination of the FISA materials in the Sealed Appendix will demonstrate that the Government satisfied FISA's requirements to obtain orders for electronic surveillance and physical search, that the information obtained pursuant to FISA was lawfully acquired, and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

Even if this Court were to determine that the FISA information was not lawfully acquired or that the electronic surveillance and physical search were not made in conformity with an order of authorization or approval, the FISA evidence would nevertheless be admissible under the good faith exception to the exclusionary rule articulated in *Leon*. 468 U.S. 897 (1984); s*ee also Ning Wen*, 477 F.3d at 897 (stating that the *Leon* good-faith exception applies to FISA orders); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8.

Respectfully submitted,

JUSTIN E. HERDMAN
United States Attorney

By: /s/ Matthew W. Shepherd
Matthew W. Shepherd
Assistant U.S. Attorney
Telephone: (216) 622-3859

/s/ Rebecca Magnone
Rebecca Magnone
Trial Attorney
National Security Division
U.S. Department of Justice

/s/ Chad M. Davis
Chad M. Davis
Attorney-Advisor
National Security Division
U.S. Department of Justice

Attorneys for The United States of America

CERTIFICATE OF SERVICE

I hereby certify that on September 29, 2017, a copy of the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Matthew W. Shepherd
Matthew W. Shepherd
Assistant United States Attorney
Ohio Reg. No. 0074056
801 W. Superior Ave.
Suite 400
Cleveland, Ohio 44113
(216) 622-3859
(216) 522-7358 fax
Matthew.shepherd@usdoj.gov